

BEFORE THE BOARD OF COUNTY COMMISSIONERS  
OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF APPROVING       )  
POLICIES IN COMPLIANCE WITH THE   )  
HEALTH INSURANCE PORTABILITY &   )  
ACCOUNTABILITY ACT OF 1996 FOR    )  
USE AT THE LANCASTER COUNTY       )  
MENTAL HEALTH CRISIS CENTER       )

RESOLUTION NO. R-13-0058

WHEREAS, pursuant to Neb. Rev. Stat. § 23-104(6) (Reissue 2012), Lancaster County has the power to do all acts in relation to the concerns of the County necessary to the exercise of its corporate powers; and

WHEREAS, pursuant to Neb. Rev. Stat. § 23-103, the powers of a county are exercised by the Board of County Commissioners; and

WHEREAS, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which, in part, calls for the administrative simplification of health care transactions and adoption of regulations ensuring the privacy and security of patient health information; and

WHEREAS, the Lancaster County Mental Health Crisis Center provides mental health care to individuals and is therefore a “covered entity” under HIPAA; and

WHEREAS, Lancaster County wishes to approve policies which allow the Mental Health Crisis Center to comply with HIPAA.




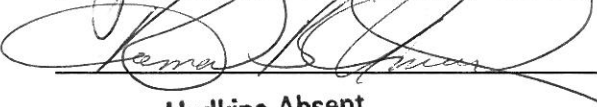
NOW, THEREFORE, BE IT RESOLVED, by the Board of County Commissioners of Lancaster County that the policies marked as Exhibit “A” and attached hereto and incorporated herein by this reference, are hereby approved.

DATED this 17 day of September, 2013, at the County-City Building, Lincoln,  
Lancaster County Nebraska.

BY THE BOARD OF COUNTY  
COMMISSIONERS OF LANCASTER  
COUNTY, NEBRASKA

APPROVED AS TO FORM  
this 17 day of  
September, 2013.

  
for JOE KELLY  
County Attorney

  
  
  
  
Hudkins Absent

## **NOTICE OF PRIVACY PRACTICES**

**THIS NOTICE DESCRIBES HOW MEDICAL AND DRUG AND ALCOHOL RELATED INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

The Lancaster County Mental Health Crisis Center is required by law to maintain the privacy of your health information and to provide you with notice of our legal duties and privacy practices with respect to your health information. Information regarding your health care, including payment for health care, is protected by two federal laws: the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §1320d *et seq.*, 45 C.F.R. Parts 160 and 164, and the Confidentiality Law, 42 U.S.C. §290dd-2, 42 C.F.R. Part 2. Under these laws, the Mental Health Crisis Center may not say to a person outside the Mental Health Crisis Center that you attend a program, nor may we disclose any information identifying you as an alcohol or drug abuser, or disclose any other protected information except as permitted by federal law. We must follow the privacy practices contained in this notice. However, we reserve the right to change the privacy practices described in this notice, in accordance with the law. A current notice will be available and posted at all times at the Mental Health Crisis Center.

### **USE AND DISCLOSURE OF YOUR HEALTH INFORMATION ONLY WITH YOUR AUTHORIZATION:**

Uses and disclosures of your health information will be made only with your written authorization. We must obtain your written authorization before we can disclose information about you for payment purposes. For example, we must obtain your written authorization before we can disclose information to your health insurer in order to be paid for services. Generally, you must also sign a written authorization before we can share information for treatment purposes or for health care operations.

### **USE AND DISCLOSURE OF YOUR HEALTH INFORMATION WITHOUT YOUR WRITTEN AUTHORIZATION:**

Federal law permits us to use and disclose information about you without your written permission in the following instances:

1. To persons or organizations known as business associates, who provide services for us under contract. We require our business associates to protect the medical information we provide to them.
2. To qualified personnel for research.
3. To qualified personnel for audit or program evaluations.
4. To report a crime committed by you on the Crisis Center premises or against Crisis Center personnel.
5. To medical personnel in a medical emergency situation.
6. To appropriate authorities to report suspected child abuse or neglect.
7. As allowed by a court order.

### **YOU HAVE SEVERAL RIGHTS WITH REGARD TO YOUR HEALTH INFORMATION:**

**Right to Inspect and Copy:** You have the right to inspect and obtain a copy of your health information. However, this right does not apply to psychotherapy notes; information gathered in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding; and protected health information that is subject to law that prohibits access to protected health information. You may be charged a reasonable fee for a copy of your records.

In some circumstances you may have the right to receive this information in an electronic copy sent to an entity or individual you have clearly, specifically, and conspicuously designated.

You have the right to request records in an electronic form and format. If records are not available in the form and format you request, we will work with you to find an agreeable form and format. If you decline any of the electronic

formats that are available, we will provide a paper copy as an option. If a portion of a record is maintained in paper, such portion does not have to be converted to an electronic format.

**Right to Request to Correct or Amend:** If you believe your health information is incorrect, you may ask us to correct or amend the information. Your request must be made in writing and must include a reason for the correction or change. If we did not create the health information that you believe is incorrect, or if we disagree with you and believe your health information is correct, we may deny your request.

**Right to Restrict Access:** You have the right to ask for restrictions on how your health information is used or disclosed for treatment, payment and health care operations. Your request must be in writing and must include what information you want to limit; whether you want to limit our use, disclosure or both; and to whom you want the limits to apply. We are not legally required to agree with your requested restriction(s) unless (1) your request is to restrict disclosures to health plans; (2) your request only limits disclosures made for the purpose of carrying out payment or health care operations; (3) the request only limits disclosures relating to health care items or services for which you, or another person on your behalf other than the health plan, have paid Lancaster County out of pocket in full; and (4) the disclosure is not otherwise required by law.

**Right to Request Confidential Communications:** You have the right to ask that we communicate your health information to you using alternative means or an alternative location. For example, you may wish to receive information about your health status in a special, private room or through a written letter sent to a private address. We will accommodate reasonable requests.

**Right to an Accounting of Disclosures:** You have the right to ask that we provide you with a list of the disclosures we have made of your health information in the six years prior to the date on which the accounting is requested. This list will not include disclosures made for treatment, payment or health care operations. This list will not include disclosures made to you or your legal representative, law enforcement/corrections, regarding inmates, certain health oversight activities, our directory, national security or pursuant to your authorization.

In some circumstances, if we maintain an electronic health record about you, you may have the right to receive an accounting of disclosures, for the last three years, which were made for treatment, payment or healthcare operations purposes.

**Right to Receive Notification of Certain Breaches:** You have the right to receive a notification from Lancaster County in certain situations. Generally, you will receive this notification if we become aware that (1) your personal health information has been accessed, disclosed, or used in violation of federal laws, and your information was not secured according to federal standards; and (2) we determine that the improper access, disclosure, or use could cause significant financial harm to you, harm to your reputation, or cause other harm to you. The notification we send will contain important information about the improper access, disclosure or use and where you can obtain further information.

**Right to Revoke Your Authorization:** If you sign an authorization form, you may withdraw your authorization at any time, as long as your withdrawal is in writing.

**Right to a Paper Copy of this Notice:** You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time.

**Complaints:** If you believe your privacy rights have been violated, you may file a complaint with us and/or with the Secretary of the U.S. Department of Health and Human Services in Washington, D.C. We will not retaliate against you for filing such a complaint. In addition, violation of 42 C.F.R. Part 2 is a reportable crime. Suspected violations may be reported to the United States Attorney in the district where the violation occurred.

If you have any questions or concerns regarding your privacy rights, the information in this notice, or if you wish to file a complaint, please contact the following individual for information:

Mental Health Crisis Center  
ATTN: HIPAA Privacy Officer  
2201 S. 17 St.  
Lincoln, NE 68504  
402-441-8276

This Notice of Privacy Practices is effective September 23, 2013.

#### ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

I hereby acknowledge that I received a copy of this Notice of Privacy Practices.

---

Patient's/Personal Representative's Signature

---

Date

---

Crisis Center's staff should complete if Acknowledgement is not signed:

1. Does the patient have a copy of the Notice form? ☐ YES ☐ NO
2. Please explain why the patient was unable to sign an acknowledgement for and the Crisis Center's efforts in trying to obtain the patient's signature:

---

---

This Notice of Privacy Practices is effective September 13, 2013, replacing Notice of Privacy Practices issued April. 14, 2003.

## **MENTAL HEALTH CRISIS CENTER**

### **GENERAL SECURITY POLICY**

**Effective Date: Sept. 13, 2013**

**References: CARF 1E3**

**Issue Date: Sept. 13, 2013**

### **HIPAA Regulations**

#### **POLICY:**

The Mental Health Crisis Center is committed to protecting electronic protected health information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent changes to that Act. To comply with the HIPAA Security Regulations the following policy is established:

1. The Mental Health Crisis Center will:
  - a. Ensure the confidentiality, integrity and availability of all ePHI created, received, maintained and transmitted;
  - b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
  - c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
  - d. Ensure compliance with the Security Regulations by its workforce.
2. Lancaster County has designated Information Services as the Security Official. Lancaster County HIPAA Security Policies can be found on the Lancaster County webpages.
3. The Mental Health Crisis Center Privacy and Security Officer (the Director) is responsible for ensuring:
  - a. Compliance with the Lancaster County HIPAA Security Policies and Procedures;
  - b. Maintaining the confidentiality of all ePHI for which the Mental Health Crisis Center is responsible; and
  - c. Assuring all workforce members receive appropriate HIPAA training.
4. The Mental Health Crisis Center HIPAA Officer is responsible for receiving, documenting and processing complaints filed by individuals regarding the handling of ePHI. All complaints will be reported to the Lancaster County HIPAA Security Officer and the Mental Health Crisis Center HIPAA Officer who will ensure that a complaint is promptly and properly investigated, documented and handled.
5. The Mental Health Crisis Center will train workforce members regarding these policies. The Mental Health Crisis Center will ensure that workforce members will be appropriately disciplined and sanctioned for violating the Lancaster County HIPAA Security Policies. The Mental Health Crisis Center will refrain from intimidating or retaliating against any person for exercising his/her rights under the HIPAA Security Regulations for reporting any concern, issue or practice that such person believes to be in violation of these Regulations or the Lancaster County HIPAA Security Policies and

Procedures. The Mental Health Crisis Center will not require any person to inappropriately waive any rights to file a complaint with the Department of Health and Human Services.

6. For purposes of the Lancaster County HIPAA Security Policies, workforce members include all full and part-time employees, volunteers, contractors, temporary workers and any others who have been granted role-based access to information assets and systems.
7. Mental Health Crisis Center workforce members are responsible for being aware of, and complying with the Lancaster County HIPAA Security Policies.

## **MENTAL HEALTH CRISIS CENTER**

### **HIPAA SECURITY POLICY**

**Effective Date: Sept. 13, 2013**

**References: CARF 1E3**

**Issue Date: Sept. 13, 2013**

### **HIPAA Regulations**

#### **POLICY:**

To ensure the Mental Health Crisis Center is in compliance with all applicable HIPAA security regulations, the following procedures are established:

1. All staff members are granted building access by proper I.D., appropriate keys, and check in procedures.
2. Medical records room access is limited to staff with a role-based need to access client records. Doors are locked when not staffed by record management personnel. All client records will be returned to Medical Records after completion of the discharge processes.
3. Mental Health Crisis Center staff members, students, and peer workers are issued photo ID's for the purpose of identification in the work environment. Photo ID's must be worn while at work.
4. Visitors and maintenance employees or contractors will sign in to ensure control of Mental Health Crisis Center access. Visitors will be escorted to their specified room or staff member office, and escorted out at the end of their visit.
5. Clients are not allowed access to client accounts, the staff mailroom, or the Medical Records room.
6. Only role-based approved professional and support staff members will have access to confidential protected health information. Such information shall be protected in secured, locked, controlled rooms/files/cabinets, and electronic protected health information shall be protected by computer security.
7. Property Management maintains and has all records regarding the Mental Health Crisis Center doors, locks, access hardware control electronics and records, heat and humidity sensors, and controls.
8. The Mental Health Crisis Center Director, along with the building maintenance personnel, will check and help maintain fire extinguishers, alarms, and smoke detectors.



## **MENTAL HEALTH CRISIS CENTER**

**HIPAA OFFICER**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

### **POLICY:**

The Mental Health Crisis Center is committed to protecting electronic protected health information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent changes to that Act.

Designation of HIPAA Privacy and Security Liaison:

HIPAA Privacy and Security Liaison:	Scott Etherton, Director
Address:	2201 S. 17 St. Lincoln, Nebraska 68502
Phone:	402-441-8276

The Mental Health Crisis Center HIPAA Privacy and Security Liaison is responsible for ensuring that the Mental Health Crisis Center:

- Complies with Lancaster County HIPAA Security Policies and Procedures;
- Works with Mental Health Crisis Center staff maintain the confidentiality of all protected health information for which they are responsible; and
- Assists in training all Mental Health Crisis Center staff regarding HIPAA rules and regulations.

## **MENTAL HEALTH CRISIS CENTER**

### **WORKFORCE SECURITY POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center is committed to protecting electronic protected health information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent changes to that Act. The purpose of this Policy is to implement procedures to ensure all members of the workforce have appropriate access to ePHI and to prevent access to those who do not need such information.

The Act established guidelines for determining workforce member access to ePHI based upon roles. This Policy is established in compliance with those guidelines.

1. The Director, or his/her designee, shall determine the necessary and appropriate level of access to ePHI for workforce members. This determination shall be based on specific requirements to fulfill job responsibilities, and includes access to both electronic and non-electronic PHI. The Director shall maintain a current list of access levels for all workforce members.
2. No workforce member's access rights shall be made or modified without formal documented approval from the Director or his/her designee.
3. If job responsibilities change for a workforce member the Director, or his/her designee, shall reevaluate access and make appropriate changes as necessary. All such determinations shall be communicated to Information Services and eBHIN (Eastern Nebraska Behavioral Health Information Network) by the Director or his/her designee.
4. Any workforce member who successfully or unsuccessfully attempts to gain access to ePHI for which they are not authorized shall be subject to disciplinary actions up to and including termination.
5. The Director, or his/her designee, shall conduct periodic audits to determine whether actual access to ePHI by workforce members is in compliance with the established requirements as determined in this policy. This shall be done at least annually.
6. In the event of termination or transfer to another position the Director, or his/her designee, shall ensure that all existing access is terminated. The Director, or his/her designee, will also determine if any other precautionary measures are to be taken.
7. To terminate access the Director, or his/her designee, shall notify Information Services and eBHIN.

## **MENTAL HEALTH CRISIS CENTER**

### **INFORMATION ACCESS POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center is committed to protecting electronic protected health information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent changes to that Act, and as such has developed this Policy to ensure that access to ePHI is properly authorized.

#### **1. Access Authorization**

- A. The Mental Health Crisis Center has established procedures for granting access to ePHI through a workstation, transaction, program or process. Procedures include:
  - i. Director, or his/her designee, is responsible for authorizing access to systems and networks containing ePHI for all Mental Health Crisis Center employees;
  - ii. Mental Health Crisis Center employees are not permitted to authorize their own access to ePHI or be granted authorization from another supervisor; and
  - iii. The Director, or his/her designee, is responsible for ensuring that access to ePHI granted to each employee is the minimum necessary access required for the job role and responsibilities.

#### **2. Access Establishment and Modification**

- A. The Director, or his/her designee, is responsible for periodically reviewing access to ePHI granted to each of the Mental Health Crisis Center employees and for modifying such access as appropriate.
- B. Information Services is responsible for security on networks, servers and systems.
- C. The Mental Health Crisis Center has established procedures for terminating access to ePHI through a workstation, transaction, program or process. Procedures include the following:
  - i. If a workforce member's employment or services are terminated the Director, or his/her designee, is responsible for ensuring that all such workforce member's accounts to access ePHI are terminated; and
  - ii. If a workforce member's employment or services are terminated the Director, or his/her designee, is responsible for ensuring that such workforce member's access to all facilities housing ePHI is terminated, including but not limited to access cards, keys, codes, and other facility access control mechanisms. Equipment access passwords, administrator passwords, and other common access control information should be changed when appropriate.
- D. If an employee of the Mental Health Crisis Center transfers to another department within Lancaster County, that employee's access to ePHI within the Mental Health Crisis Center must be terminated as of the date of the transfer.

## **MENTAL HEALTH CRISIS CENTER**

### **SECURITY AWARENESS AND TRAINING POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center shall establish a training methodology to provide adequate initial and ongoing training regarding the risks associated with the access, use and disclosure of ePHI. Therefore, this Policy is enacted.

#### **1. Security Training Program**

- A. The Mental Health Crisis Center shall provide ongoing information security awareness and education for all members of its workforce. This shall cover information security basics, associated policies, procedures, and workforce member responsibilities.
- B. The Mental Health Crisis Center shall ensure that workforce members are aware of information security policies, procedures, and guidelines and have access to current versions of the same.
- C. The Mental Health Crisis Center shall inform new employees, temporary workers and volunteers of the requirements of information security and their role in protecting valuable and sensitive information. This will occur during new employee orientation. Annual reminders will occur in connection with annual performance evaluations and more often if deemed necessary by the Director.
- D. Employees, temporary workers and volunteers shall acknowledge they have been informed and are aware of Lancaster County's HIPAA Security Policies and their role in regard to those Policies by signing the Employee Acknowledgement and Receipt of Lancaster County HIPAA Privacy and Security Policies and Procedures Form.
- E. The Mental Health Crisis Center shall hold an annual awareness and education session to review information security basics and current information security policies with workforce members. This can be in conjunction with any annual privacy awareness and education session.

#### **2. Security Events**

- A. In the event of a security event Information Services will provide information on countermeasures to be taken to reduce the negative impact of such event.
- B. Information Services is responsible to develop and implement procedures to detect and guard against malicious code and any other computer program or code designed to interfere with normal operation of a system. Information Services is responsible for the security of the County network, databases, email, etc.

- C. Information Services will be responsible for ensuring that any system which has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

### 3. Password Management

- A. All workforce members who access the Lancaster County network or applications that contain ePHI shall be supplied with a unique user id and password to access said systems.
- B. All passwords used to gain access to any network or applications that contain ePHI must be of sufficient complexity to ensure it is not easily guessed.
- C. Workforce members are responsible for the proper use and protection of their passwords.
  - i. Passwords must not be disclosed to other workforce or family members
  - ii. Appropriate identification or verification shall be made on all persons representing themselves as service providers needing temporary access to machines that have access to any network
  - iii. Passwords shall not be written down, posted or held in a conspicuous, easily found location
  - iv. A password will be changed immediately if it is suspected of being disclosed
  - v. Workforce members should refuse all offers by software and/or internet sites to automatically login
- D. Passwords will be changed per instructions from Information Services or eBHIN.

## **MENTAL HEALTH CRISIS CENTER**

### **SECURITY INCIDENT POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center is committed to protecting Protected Health Information, both in electronic and paper form, and has developed this Policy to identify and respond to HIPAA security incidents and violations.

1. All incidents, threats or violations that affect or may affect the confidentiality, integrity, or availability of ePHI must be reported and responded to using the following procedure:
  - a. Any workforce member suspecting a security incident shall immediately notify the Director or their supervisor. If the incident appears to be computer virus/malicious code/a network or system attack Information Services should also be notified immediately.
  - b. To the fullest extent possible, such employee shall provide the date, time and incident specifics. This information will be treated as confidential information.
2. The Director, or a supervisor if the Director is unavailable, shall immediately contact the Lancaster County HIPAA Officer and, if appropriate, Information Services.
  - a. The Director, or supervisor, shall document the incident to the fullest extent possible.
  - b. The County HIPAA Officer, Director, and Information Services, if appropriate, shall investigate to determine if a breach has occurred, take the necessary and required actions to limit the damage and handle the situation.

## **MENTAL HEALTH CRISIS CENTER**

### **CONTINGENCY OPERATIONS POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center is committed to minimizing the impact of emergencies or other events that negatively impact operations.

Information Services maintains a plan to recover operations and protect data due to an emergency or disaster.

The Mental Health Crisis Center has established procedures to continue critical business operations during an emergency. (Refer to the Disaster Recovery Plan)

- These procedures include provisions for the continued protection of ePHI during the emergency period
- These procedures are documented and reviewed on a regular basis and are easily available to necessary personnel at all times.

## **MENTAL HEALTH CRISIS CENTER**

### **FACILITY ACCESS CONTROLS POLICY**

**Effective Date: Sept. 13, 2013**

**Issue Date: Sept. 13, 2013**

#### **POLICY:**

The Mental Health Crisis Center has adopted this policy to limit physical access to its electronic information systems and the facility in which such systems are housed, while still ensuring that proper authorized access is followed.

#### **1. Contingency Operations**

- A. During a disaster the Disaster Recovery Plan will be implemented. The Plan specifies how facility access controls are to be handled and how information systems will be accessed.

#### **2. Facility Security Plan**

- A. The Director or his/her designee is responsible for developing, implementing and maintaining this Facility Access Controls Policy. Details related to access controls and validation are as follows:

Validation of the identity of persons physically present at the facility includes the use of workforce member ID badges; visitor sign-in, ID badges and escorts; and patient escorts where applicable.

#### **3. Access Control and Validation Procedures**

- A. The Director or his/her designee will use role-based criteria to control and validate workforce member's access to systems and facilities where PHI (both electronic and in paper form) is maintained or available for review or stored.
- B. Facilities where PHI is available will have appropriate physical access controls to limit access.
- C. The Director or his/her designee will work with facility management to ensure all environmental controls are appropriate.

#### **4. Maintenance Records**

- A. The Director or his/her designee, along with the facility management, will document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.



## MENTAL HEALTH CRISIS CENTER

### POLICY FOR MHCC REGARDING PHI LEAVING THE OFFICES

Effective Date: Sept. 13, 2013

Issue Date: Sept. 13, 2013

#### POLICY:

It is a requirement for HIPAA covered entities to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from the offices and to guard against impermissible disclosures, potentially violating provisions of the HIPAA Privacy Rule.

Therefore, following is the policy of the Mental Health Crisis Center (MHCC) relating to the removal of PHI from the CMHC offices:

- When any paper documents are removed from the offices, the employee taking those documents must first receive permission to take the documents, then note the information on the Transfer Form.
- Paper documents must be secured at all times. They are not to be left in any vehicle. The documents should be returned at the end of the working day, but if not, they are not to be left overnight in any vehicle and must be kept away from others in the residence.
- Paper documents and forms leaving the office must not contain personal information, such as social security numbers, date of birth, client number, insurance company and policy number, mental health diagnosis, treatment plans, and the like. In all cases, personal identifying information must not be added to the form until after the document is back in the CMHC offices.
- Appointment books must not contain information that could potentially be harmful to clients. Limit information in such books to first name or initial, phone number, and, if necessary, address. Do not write any treatment or visit notes in the appointment book. Information that can be found in a phone book is not considered sensitive, but when such information is contained in any document that includes a list of clients of the MHCC it becomes sensitive information.
- Mobile devices information should be handled in the same manner as appointment books. Additionally, no pictures of clients are to be taken with any mobile device. No PHI is to be carried on any cell phone-like device. This applies to both personal and MHCC cell phone-like devices.
- Employees of the MHCC are asked to not access any client's social media pages on any cell phone-like device or on their work or home computers.
  - An employee removing PHI from the MHCC offices in any electronic format (flash drive, CD, etc.) must first receive permission from his/her supervisor to do so.
  - NOTE: Lancaster County is required to guarantee your home computer is as well-protected as the County's network. We cannot make that guarantee. Therefore, if you work from home you must work on the County's network. Please be sure you are set

up appropriately to do so, and you must let the Director know that you are doing work from your home computer. Do not save any client information on your home computer. If you have questions about how to be certain you have totally deleted the information, contact Information Services.

- As with paper documents, PHI removed from the offices in any electronic format must be safeguarded. Flash drives, CD's, etc. must not be left in a vehicle and should be returned to the office at the end of the working day. If that is not possible, the devices must be kept in the residence overnight and kept away from those who are not authorized to have access to the information contained on the device.
- Any portable electronic device must be password protected. Please contact IS to ensure such devices set up properly. Such portable devices must be the property of Lancaster County, not the employee. In most situations, PHI should NOT be on any portable electronic device.